Babuk ransomware is back, uses new version on corporate networks

By Ionut Ilascu

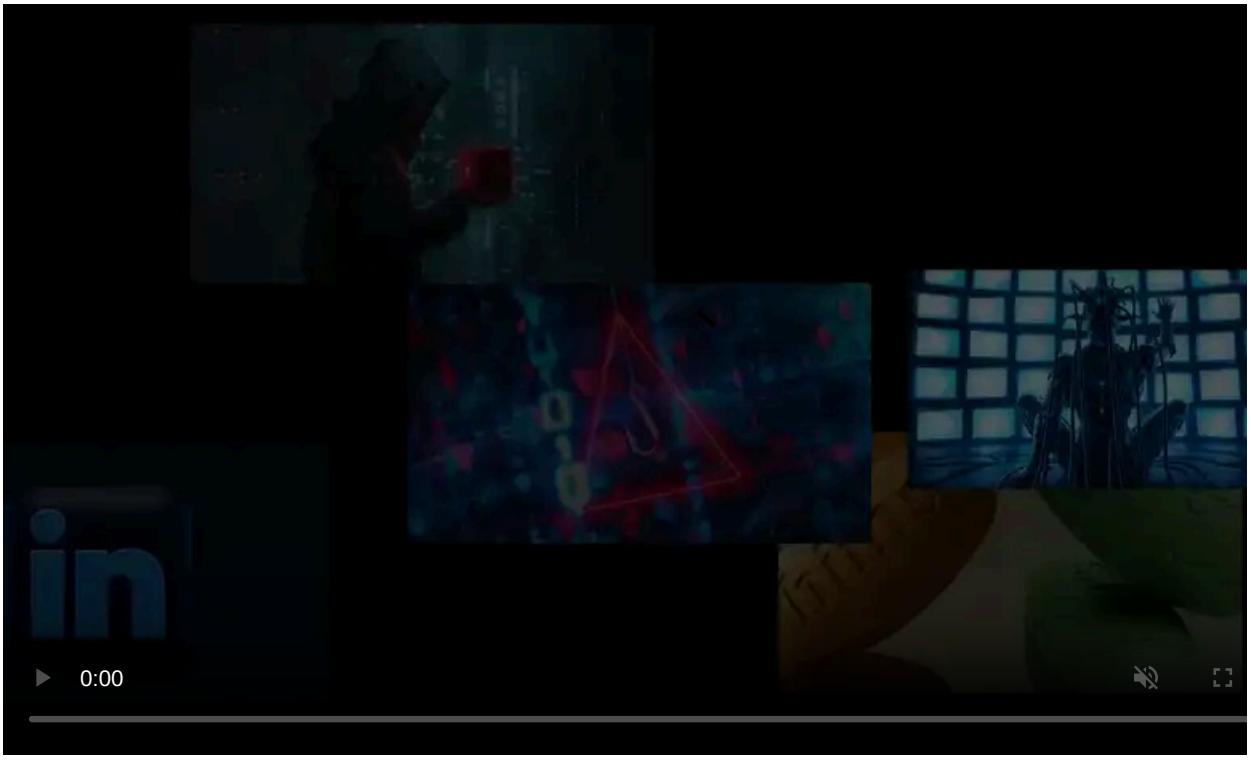
Published: 2021-07-01 · Archived: 2026-04-05 18:50:37 UTC

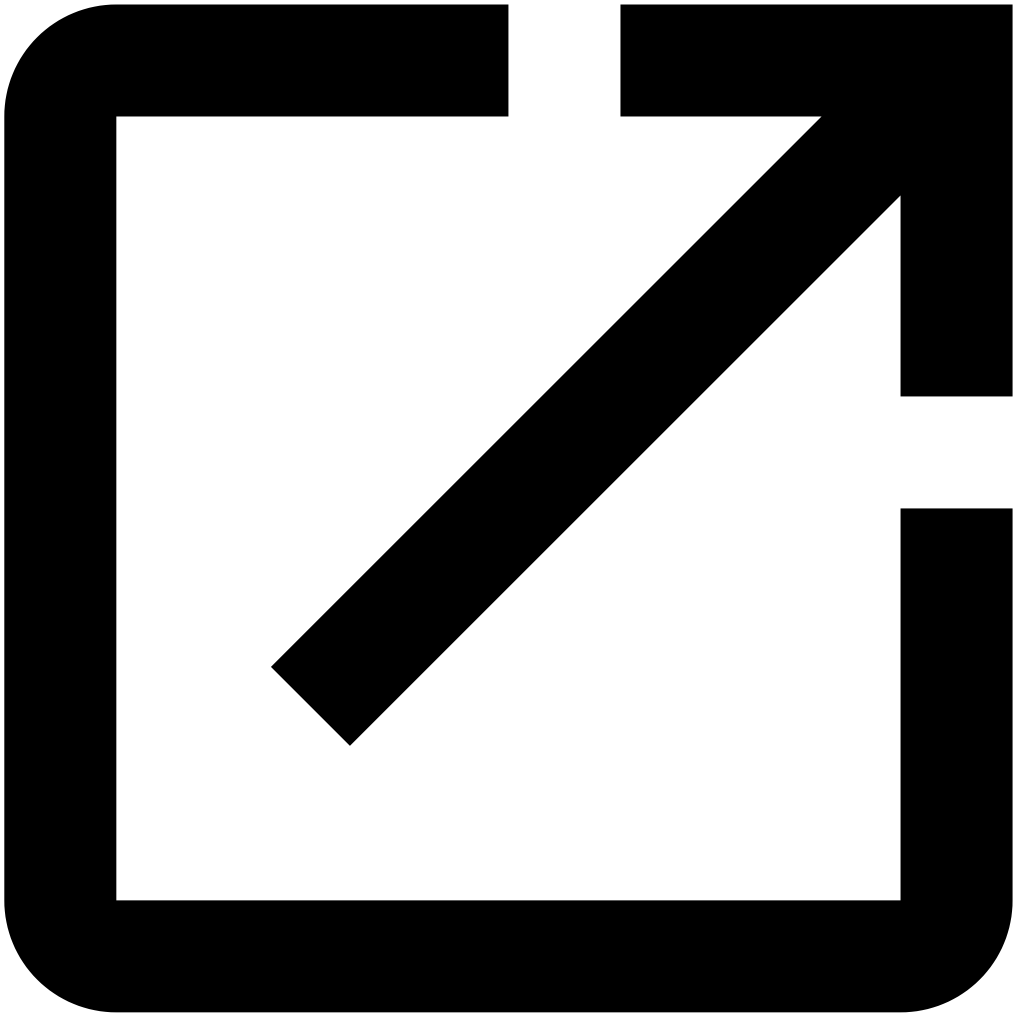
After announcing their exit from the ransomware business in favor of data theft extortion, the Babuk gang appears to have slipped back into their old habit of encrypting corporate networks.

The criminals are currently using a new version of their file-encrypting malware and have moved the operation to a new leak site that lists a handful of victims.

Gang's still in the game

The Babuk ransomware group became known at the beginning of the year but the gang says that their attacks had started in mid-October 2020, targeting companies across the world and demanding ransoms typically between $60,000 and $85,000 in bitcoin cryptocurrency. In some cases, victims were asked hundreds of thousands for data decryption.


0:00



One of their most publicized victims is the Washinton DC's Metropolitan Police Department (MPD). This attack likely pushed the threat actor into announcing its retirement from the ransomware business only to adopt another extortion model that did not include encryption.

The gang also announced plans to release their malware so that other cybercriminals could start a ransomware-as-a-service operation. The threat actor kept its promise and published its builder, a tool that generates customized ransomware.

Security researcher Kevin Beaumont found it on VirusTotal and shared the information to help the infosec community with detection and decryption.

After shutting down in April, the gang took the name PayLoad Bin, but their leak site shows little activity. Instead, a new leak site emerged on the dark web carrying the Babuk ransomware markings.

The site lists fewer than five victims that refused to pay the ransom and that they have been attacked with a second version of the malware.

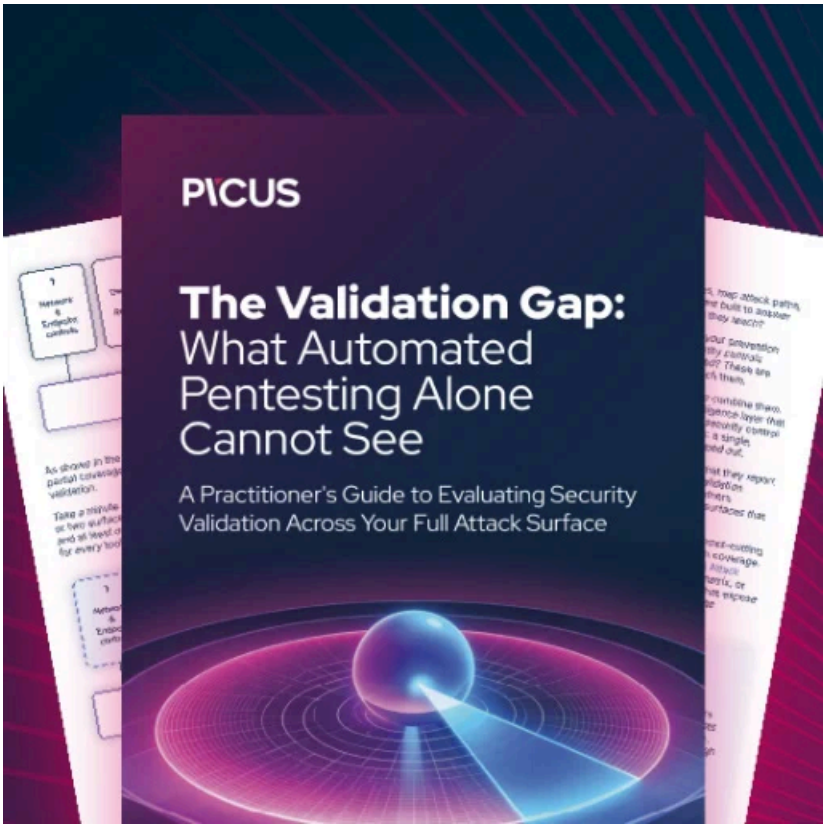
It appears that Babuk has not given up the encryption-based extortion game. They released only the old version of their malware and created a new one to get back into the ransomware business.

The gang made this clear in a comment to our article about a rush of ransomware attacks that used the leaked Babuk builder and demanded .006 bitcoins (currently about $200) - clearly showing that it’s not the original group using it.

It appears that the Babuk gang is not ready to give up the file-encryption activity and will continue to focus on corporate networks for larger payments.

It is unclear what drove the group to return to their old practices but given how empty the PayLoad Bin leak site is, one can speculate that data theft extortion did not go too well.

Also, it remains unknown at the moment if the new Babuk operation has behind it the same members that attacked Washinton DC's Metropolitan Police Department or this incident produced a split.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/babuk-ransomware-is-back-uses-new-version-on-corporate-networks/